Глава IX

Расширения колец

В этой главе слово „кольцо" будет обозначать „коммутативное кольцо".

§ 1. Целые расширения колец

В гл. VII и VIII мы изучали алгебраические расширения полей. По целому ряду причин желательно исследовать также алгебраические расширения колец. Например, данный многочлен с целыми коэффициентами, скажем $X^5 - X - 1$, можно привести по модулю любого простого числа p и получить таким образом многочлен с коэффициентами в конечном поле. В качестве другого примера рассмотрим многочлен

$$X^n + s_{n-1}X^{n-1} + \ldots + s_0,$$

где $s_{n-1}, \ldots, s_0$ алгебраически независимы над полем k. Этот многочлен имеет коэффициенты в $k[s_0, \ldots, s_{n-1}]$, а после подстановки вместо $s_0, \ldots, s_{n-1}$ элементов из k получается многочлен с коэффициентами в k. В общем можно получать информацию о многочленах, беря гомоморфизм кольца, в котором лежат их коэффициенты. Эта глава посвящена краткому описанию основных фактов, касающихся многочленов над кольцами.

Пусть A — кольцо и M — A-модуль. Мы будем говорить, что модуль M *точный*, если равенство $aM = 0$, $a \in A$, возможно только при $a = 0$. Отметим, что A является точным модулем над собой, поскольку A содержит единичный элемент. Кроме того, если $A \neq 0$, то точный модуль над A не может быть модулем, состоящим только из нуля.

Пусть A — подкольцо кольца B и $\alpha \in B$. Следующие условия эквивалентны:

ЦЕЛ 1. Элемент α есть корень многочлена

$$X^n + a_{n-1}X^{n-1} + \ldots + a_0$$

степени $n \geqslant 1$ с коэффициентами $a_i \in A$. (Существенным моментом здесь является то, что старший коэффициент равен 1.)

ЦЕЛ 2. Подкольцо $A[\alpha]$ — конечно порожденный A-модуль.

ЦЕЛ 3. Существует точный модуль над $A[\alpha]$, являющийся конечно порожденным A-модулем.

Докажем их эквивалентность. Предположим, что выполняется ЦЕЛ 1. Пусть $g(X)$ — многочлен из $A[X]$ степени $\geqslant 1$ со старшим коэффициентом 1, для которого $g(\alpha)=0$. Если $f(X) \in A[X]$, то

$$f(X)=q(X)g(X)+r(X),$$

где q, $r \in A[X]$ и $\deg r < \deg g$. Следовательно, $f(\alpha)=r(\alpha)$ и мы видим, что если $\deg g=n$, то $1, \alpha, \ldots, \alpha^{n-1}$ являются образующими $A[\alpha]$ как модуля над A.

Уравнение $g(X)=0$, где g — многочлен описанного выше вида, для которого $g(\alpha)=0$, называется *целым уравнением* для α над A.

Предположим, что выполняется ЦЕЛ 2. Тогда в качестве точного модуля мы можем взять само кольцо $A[\alpha]$.

Предположим, что выполняется ЦЕЛ 3, и пусть M — точный модуль над $A[\alpha]$, конечно порожденный над A, скажем, элементами $w_1, \ldots, w_n$. Так как $\alpha M \subset M$, то существуют элементы $a_{ij} \in A$, такие, что

$$\begin{aligned} \alpha w_1 &= a_{11}w_1 + \ldots + a_{1n}w_n, \\ &\ldots\ldots\ldots\ldots\ldots \\ \alpha w_n &= a_{n1}w_1 + \ldots + a_{nn}w_n. \end{aligned}$$

Перенося $\alpha w_1, \ldots, \alpha w_n$ в правые части этих уравнений, мы приходим к заключению, что определитель

$$d=\begin{vmatrix} \alpha-a_{11} & & & \\ & \alpha-a_{22} & & -a_{ij} \\ & & \ddots & \\ -a_{ij} & & & \alpha-a_{nn} \end{vmatrix}$$

аннулирует M: $dM=0$. (Это будет доказано в главе, в которой мы рассматриваем определители.) Так как модуль M точный, то должно выполняться равенство $d=0$. Следовательно, α есть корень многочлена

$$\det|X\delta_{ij}-a_{ij}|,$$

дающего целое уравнение для α над A.

Элемент α, удовлетворяющий трем предыдущим условиям ЦЕЛ 1, 2, 3, называется *целым* над A.

Предложение 1. *Пусть A — целое кольцо, K — его поле частных и α — алгебраический элемент над K. Тогда в A существует элемент $c \neq 0$, такой, что $c\alpha$ — целый элемент над A.*

Доказательство. Имеем уравнение

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0,$$

где $a_i \in A$ и $a_n \neq 0$. Умножим его на a_n^{n-1}. Тогда

$$(a_n\alpha)^n + \ldots + a_0 a_n^{n-1} = 0$$

будет целым уравнением для $a_n\alpha$ над A.

Пусть A, B — подкольца кольца C, и пусть $\alpha \in C$. Если α — целый элемент над A и $A \subset B$, то тем более α — целый элемент над B. Таким образом, целость элемента сохраняется при подъеме.

Пусть B — кольцо, содержащее A в качестве подкольца. Мы будем говорить, что B — *целое* над A, если всякий элемент из B является целым над A.

Предложение 2. *Если B — целое кольцо над A, конечно порожденное как A-алгебра, то B конечно порождено и как A-модуль.*

Доказательство. Это предложение можно доказывать индукцией по числу кольцевых образующих и, таким образом, учитывая наличие башни

$$A \subset A[\alpha_1] \subset A[\alpha_1, \alpha_2] \subset \ldots \subset A[\alpha_1, \ldots, \alpha_n] = B,$$

предполагать, что $B = A[\alpha]$ для некоторого элемента α, целого над A. Но, как мы уже видели, в этом случае наше утверждение верно (это составляет часть определения целости).

Так же как для расширений полей, мы можем говорить, что класс $\mathscr{C}$ расширений колец $A \subset B$ является *отмеченным*, если он удовлетворяет аналогичным свойствам, а именно:

(i) Пусть $A \subset B \subset C$ — башня колец. Расширение $A \subset C$ тогда и только тогда принадлежит $\mathscr{C}$, когда $A \subset B$ принадлежит $\mathscr{C}$ и $B \subset C$ принадлежит $\mathscr{C}$.

(ii) Если $A \subset B$ принадлежит $\mathscr{C}$ и C — любое расширение кольца A, причем B, C оба являются подкольцами некоторого кольца, то $C \subset B[C]$ принадлежит $\mathscr{C}$. (Отметим, что $B[C] = C[B]$ есть наименьшее кольцо, содержащее и B, и C.)

Как и для полей, мы в качестве формального следствия из (i) и (ii) получаем, что выполняется также и свойство

(iii) Если $A \subset B$ и $A \subset C$ принадлежат $\mathscr{C}$, причем B, C — подкольца некоторого кольца, то $A \subset B[C]$ принадлежит $\mathscr{C}$.

Предложение 3. *Целые расширения колец образуют отмеченный класс.*

Доказательство. Пусть $A \subset B \subset C$ — башня колец. Если C — целое над A, то ясно, что B — целое над A и C — целое над B.

Обратно, предположим, что каждый этаж в башне целый. Пусть $\alpha \in C$. Тогда α удовлетворяет целому уравнению

$$\alpha^n + b_{n-1}\alpha^{n-1} + \ldots + b_0 = 0,$$

где $b_i \in B$. Положим $B_1 = A[b_0, \ldots, b_{n-1}]$. Тогда B_1, согласно предложению 2, будет конечно порожденным A-модулем и $B_1[\alpha]$ — конечно порожденным B_1-модулем. Так как $A[\alpha] \subset B_1[\alpha]$, то $B_1[\alpha]$ — точный $A[\alpha]$-модуль. Наконец, $B_1[\alpha]$ есть конечно порожденный A-модуль. Действительно, если $v_1, \ldots, v_r$ — образующие B_1 над A и $w_1, \ldots, w_s$ — образующие $B_1[\alpha]$ над B_1, то $v_i w_j$, $i = 1, \ldots, r$, $j = 1, \ldots, s$, порождают $B_1[\alpha]$ над A. Следовательно, кольцо C — целое над A. Наконец, пусть B, C — кольца, являющиеся расширениями A, причем B — целое над A. Предположим, что B, C — подкольца некоторого кольца. Тогда $C[B]$ порождается над C элементами из B, а каждый элемент из B является целым над C. То, что $C[B]$ является целым над C, непосредственно вытекает теперь из следующего предложения.

Предложение 4. *Пусть A — подкольцо кольца C. Тогда элементы из C, целые над A, образуют подкольцо в C.*

Доказательство. Если α — целый элемент над A, то $A[\alpha]$ — целое расширение A, поскольку для любого $\alpha' \in A[\alpha]$ конечно порожденный A-модуль $A[\alpha]$ является точным $A[\alpha']$-модулем. Пусть теперь α, $\beta \in C$ — целые элементы над A. Рассмотрим башню $A \subset A[\alpha] \subset A[\alpha, \beta]$. Каждый этаж в этой башне является целым, а потому, согласно первой части доказательства предложения 3, $A[\alpha, \beta]$ — целое расширение A. Следовательно, $\alpha \pm \beta$ и $\alpha\beta$ — целые элементы над A, что и доказывает наше предложение.

В условиях предложения 4 множество элементов из C, целых над A, называется *целым замыканием* кольца A в C.

Предложение 5. *Пусть B — целое кольцо над A и σ — его гомоморфизм. Тогда кольцо $\sigma(B)$ — целое над $\sigma(A)$.*

Доказательство. Пусть $\alpha \in B$ и

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$$

— целое уравнение для α над A. Применение σ дает

$$\sigma(\alpha)^n + \sigma(a_{n-1})\,\sigma(\alpha)^{n-1} + \cdots + \sigma(a_0) = 0,$$

что и доказывает наше утверждение.

Следствие. *Пусть A — целостное кольцо, k — его поле частных, E — конечное расширение над k и $\alpha \in E$ — целый элемент над A. Тогда норма и след элемента α (из E в k) являются* *целыми над A и таковы же коэффициенты неприводимого многочлена над k, соответствующего α.*

Доказательство. Для всякого вложения σ поля E над k элемент $\sigma\alpha$ является целым над A. Так как норма — это произведение элементов $\sigma\alpha$ по всем таким σ (возведенное в степень, равную некоторой степени характеристики), то норма — целый элемент над A. Аналогичное верно для следа и для коэффициентов многочлена $\operatorname{Irr}(\alpha, k, X)$, которые являются элементарными симметрическими функциями от его корней.

Пусть A — целостное кольцо и k — его поле частных. Мы будем говорить, что A *целозамкнуто*, если оно совпадает со своим целым замыканием в k.

Предложение 6. *Всякое факториальное кольцо A целозамкнуто.*

Доказательство. Предположим, что имеется дробь a/b с $a, b \in A$, целая над A, и простой элемент p в A, делящий b, но не делящий a. Тогда для некоторого целого числа $n \geqslant 1$ и $a_i \in A$

$$(a/b)^n + a_{n-1}(a/b)^{n-1} + \cdots + a_0 = 0,$$

откуда

$$a^n + a_{n-1}ba^{n-1} + \cdots + a_0b^n = 0.$$

Так как элемент p делит b, то он должен делить a^n, а следовательно, и a — противоречие.

Пусть $f\colon A \to B$ — гомоморфизм колец (A, B — коммутативные кольца). Напомним, что такой гомоморфизм называется также A-алгеброй. Мы можем рассматривать B как A-модуль. Будем говорить, что B — целое над A (относительно этого кольцевого гомоморфизма f), если B — целое над $f(A)$. Это расширение нашего определения целости полезно, так как в некоторых приложениях имеют место отклонения от обычной ситуации, а мы тем не менее хотим говорить о целости. Более точно, нам следовало бы говорить, что не B является целым над A, а что f есть *целый гомоморфизм колец* или, просто, f — *целый*. Мы будем часто использовать эту терминологию.

Некоторые из наших предыдущих предложений непосредственно дают следствия для целых гомоморфизмов колец; например, если $f\colon A \to B$ и $g\colon B \to C$ целые, то $g \circ f\colon A \to C$ целый. Однако, вообще говоря, не верно, что если $g \circ f$ целый, то целый и f.

Пусть $f\colon A \to B$ — целый гомоморфизм и S — мультипликативное подмножество в A. Тогда имеет место гомоморфизм

$$S^{-1}f\colon S^{-1}A \to S^{-1}B,$$

где, строго говоря, $S^{-1}B=(f(S))^{-1}B$ и $S^{-1}f$ определяется по формуле

$$(S^{-1}f)(x/s)=f(x)/f(s).$$

Проверка того, что это гомоморфизм, тривиальна. Имеет место коммутативная диаграмма

$$\begin{array}{ccc} B & \to & S^{-1}B \\ {\scriptstyle f}\uparrow & & \uparrow{\scriptstyle S^{-1}f} \\ A & \to & S^{-1}A \end{array}$$

горизонтальными отображениями в которой служат канонические отображения $x\longmapsto x/1$.

Предложение 7. *Пусть f: $A\to B$ — целый гомоморфизм и S — мультипликативное подмножество в A. Тогда гомоморфизм $S^{-1}f$: $S^{-1}A\to S^{-1}B$ — целый.*

Доказательство. Для $\alpha\in B$, $a\in A$ и $s\in S$ будем писать $a\alpha$ и α/s вместо $f(a)\alpha$ и $\alpha/f(s)$ соответственно. Так как всякий элемент $\alpha\in B$ — целый над $f(A)$, то имеем

$$\alpha^n+a_{n-1}\alpha^{n-1}+\dots+a_0=0,$$

где $a_i\in A$. Беря канонический образ в $S^{-1}B$ и деля почленно на s^n, получаем

$$(\alpha/s)^n+(a_{n-1}/s)(\alpha/s)^{n-1}+\dots+a_0/s^n=0;$$

это доказывает, что элемент α/s является целым над $(S^{-1}f)(S^{-1}A)$.

Предложение 8. *Пусть A — целостное и целозамкнутое кольцо, S — мультипликативное подмножество в A, $0\notin S$. Тогда $S^{-1}A$ целозамкнуто.*

Доказательство. Пусть α — элемент поля частных, целый над $S^{-1}A$. Имеем уравнение

$$\alpha^n+\frac{a_{n-1}}{s_{n-1}}\alpha^{n-1}+\dots+\frac{a_0}{s_0}=0,$$

$a_i\in A$ и $s_i\in S$. Пусть s равно произведению $s_{n-1}\dots s_0$. Тогда ясно, что элемент $s\alpha$ — целый над A и, следовательно, лежит в A. Значит, α лежит в $S^{-1}A$ и кольцо $S^{-1}A$ целозамкнуто.

Лемма Накаямы. *Пусть A — кольцо, $\mathfrak{a}$ — идеал, содержащийся во всех максимальных идеалах кольца A, и M — конечно порожденный A-модуль. Если $\mathfrak{a}M=M$, то $M=0$.*

Доказательство. Индукция по числу образующих M. Пусть, скажем, M порождается элементами $w_1, \ldots, w_n$. Существует представление

$$w_1 = a_1 w_1 + \cdots + a_n w_n,$$

где $a_i \in \mathfrak{a}$. Следовательно,

$$(1 - a_1) w_1 = a_2 w_2 + \cdots + a_n w_n.$$

Если элемент $1 - a_1$ не является единицей в A, то он содержится в некотором максимальном идеале $\mathfrak{p}$. Так как $a_1 \in \mathfrak{p}$ по предположению, то мы получаем противоречие: $1 \in \mathfrak{p}$. Следовательно, $1 - a_1$ — единица, и предыдущее равенство, разделенное на этот элемент, показывает, что модуль M может быть порожден $n - 1$ элементами, чем и завершается доказательство.

Пусть $\mathfrak{p}$ — простой идеал кольца A и S — дополнение к $\mathfrak{p}$ в A. Мы пишем в этом случае $S = A - \mathfrak{p}$. Если $f\colon A \to B$ есть A-алгебра (т. е. гомоморфизм колец), то будем писать $B_\mathfrak{p}$ вместо $S^{-1}B$. Мы можем рассматривать $B_\mathfrak{p}$ как $A_\mathfrak{p} = S^{-1}A$-модуль.

Пусть A — подкольцо в B, $\mathfrak{p}$ — простой идеал в A и $\mathfrak{P}$ — простой идеал в B. Мы будем говорить, что $\mathfrak{P}$ *лежит над* $\mathfrak{p}$, если $\mathfrak{P} \cap A = \mathfrak{p}$. В этом случае вложение $A \to B$ индуцирует вложение факторколец

$$A/\mathfrak{p} \to B/\mathfrak{P},$$

и по существу мы имеем коммутативную диаграмму

$$\begin{array}{ccc} B & \to & B/\mathfrak{P} \\ \uparrow & & \uparrow \\ A & \to & A/\mathfrak{p} \end{array}$$

в которой горизонтальные стрелки обозначают канонические гомоморфизмы, а вертикальные — вложения.

Если кольцо B — целое над A, то $B/\mathfrak{P}$ — целое над $A/\mathfrak{p}$, согласно предложению 5.

Предложение 9. *Пусть A — подкольцо в B и $\mathfrak{p}$ — простой идеал в A, причем кольцо B — целое над A. Тогда $\mathfrak{p}B \neq B$ и существует простой идеал $\mathfrak{P}$ в B, лежащий над $\mathfrak{p}$.*

Доказательство. Мы знаем, что $B_\mathfrak{p}$ — целое над $A_\mathfrak{p}$ и что $A_\mathfrak{p}$ — локальное кольцо с максимальным идеалом $\mathfrak{m}_\mathfrak{p} = S^{-1}\mathfrak{p}$, где $S = A - \mathfrak{p}$. Так как, очевидно,

$$\mathfrak{p}B_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}B_\mathfrak{p} = \mathfrak{m}_\mathfrak{p}B_\mathfrak{p},$$

наше первое утверждение достаточно доказать для случая, когда A — локальное кольцо. (Отметим, что существование простого идеала $\mathfrak{p}$

влечет, что $1 \neq 0$ и $\mathfrak{p}B = B$ тогда и только тогда, когда $1 \in \mathfrak{p}B$.) Если $\mathfrak{p}B = B$, то 1 представляется в виде линейной комбинации элементов из B с коэффициентами в $\mathfrak{p}$

$$1 = a_1b_1 + \cdots + a_nb_n,$$

где $a_i \in \mathfrak{p}$ и $b_i \in B$. Пусть $B_0 = A[b_1, \ldots, b_n]$. Тогда $\mathfrak{p}B_0 = B_0$ и B_0 — конечный A-модуль в силу предложения 2. Следовательно, $B_0 = 0$ в силу леммы Накаямы, — противоречие.

Чтобы доказать наше второе утверждение, рассмотрим следующую коммутативную диаграмму:

$$\begin{array}{ccc} B & \longrightarrow & B_{\mathfrak{p}} \\ \uparrow & & \uparrow \\ A & \longrightarrow & A_{\mathfrak{p}} \end{array}$$

Мы только что доказали, что $\mathfrak{m}_{\mathfrak{p}}B_{\mathfrak{p}} \neq B_{\mathfrak{p}}$. Следовательно, $\mathfrak{m}_{\mathfrak{p}}B_{\mathfrak{p}}$ содержится в некотором максимальном идеале $\mathfrak{M}$ кольца $B_{\mathfrak{p}}$. Переходя к прообразам, мы видим, что прообраз $\mathfrak{M}$ в $A_{\mathfrak{p}}$ есть идеал, содержащий $\mathfrak{m}_{\mathfrak{p}}$. Так как идеал $\mathfrak{m}_{\mathfrak{p}}$ максимальный, то $\mathfrak{M} \cap A_{\mathfrak{p}} = \mathfrak{m}_{\mathfrak{p}}$. Пусть $\mathfrak{P}$ — прообраз $\mathfrak{M}$ в B. Тогда $\mathfrak{P}$ — простой идеал в B. Прообраз $\mathfrak{m}_{\mathfrak{p}}$ в A есть просто $\mathfrak{p}$. Беря полный прообраз $\mathfrak{M}$ по обоим путям в диаграмме, находим

$$\mathfrak{P} \cap A = \mathfrak{p},$$

что и требовалось показать.

Предложение 10. *Пусть A — подкольцо в B, причем кольцо B — целое над A. Простой идеал $\mathfrak{P}$ в B, лежащий над простым идеалом $\mathfrak{p}$ кольца A, максимален в том и только в том случае, если $\mathfrak{p}$ максимален.*

Доказательство. Предположим, что $\mathfrak{p}$ максимален в A. Тогда $A/\mathfrak{p}$ — поле и $B/\mathfrak{P}$ — целостное кольцо, целое над $A/\mathfrak{p}$. Если $\alpha \in B/\mathfrak{P}$, то элемент α алгебраичен над $A/\mathfrak{p}$, а мы знаем, что тогда $A/\mathfrak{p}[\alpha]$ — поле. Следовательно, всякий ненулевой элемент из $B/\mathfrak{P}$ обратим в кольце $B/\mathfrak{P}$, которое поэтому является полем. Обратно, предположим, что $\mathfrak{P}$ — максимальный идеал в B. Тогда $B/\mathfrak{P}$ — поле, целое над целостным кольцом $A/\mathfrak{p}$. Если $A/\mathfrak{p}$ — не поле, то оно содержит ненулевой максимальный идеал $\mathfrak{m}$. В силу предложения 9 в $B/\mathfrak{P}$ существует простой идеал $\mathfrak{M}$, лежащий над $\mathfrak{m}$, $\mathfrak{M} \neq 0$, — противоречие.

§ 2. Целые расширения Галуа

Мы исследуем здесь взаимоотношение между теорией Галуа многочлена и теорией Галуа того же самого многочлена, приведенного по модулю простого идеала.

Предложение 11. *Пусть A — целостное кольцо, целозамкнутое в своем поле частных K; L — конечное нормальное расши-*